FortiAnalyzer - Report Performance Troubleshooting Guide

VERSION 5.2.10

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

March 07, 2018

FortiAnalyzer 5.2.10 Report Performance Troubleshooting Guide

05-5210-416126-20180307

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-04-12	Initial release.
2018-03-07	Added *Check Report and Chart Settings* section.

Troubleshooting Report Performance

This guide helps you to troubleshoot reporting and FortiView related performance issues. If your system has reporting and FortiView related performance issues, try the following methods to determine and solve the problem.

Many troubleshooting steps use CLI commands and require interpreting the results to isolate the cause of performance issues.

Group reports

Grouping reports can significantly save report generation time. Grouping reports can reduce the number of *hcache* tables, improve *auto-hcache* completion time, and improve report completion time. To see which reports are in a group, use the `execute sql-report list-schedule <ADOM>` command. To group reports, see Grouping reports in the *FortiAnalyzer Administration Guide*.

Run the same report on a difference device

Try running the same report on a different device and see if performance improves. If reports run faster on a newer device, consider upgrading your hardware. If report performance is similar on different devices, use the following sections to continue troubleshooting.

Check hardware and software status

Run `get system status`

This command shows system status such as platform type (hardware or VM), firmware version, system time, disk usage, and file system format.

Use this information to check if the hardware is overloaded. This information also helps you and customer support to quickly identify any issues and narrow down the investigation.

Following is a sample result of running this command.

```
Platform Type : FAZ3500E
Platform Full Name : FortiAnalyzer-3500E
Version : v5.2.5-build3183 160216 (GA)
Serial Number : FL99999999999999
BIOS version : 00010001
System Part-Number : P15168-01
Hostname : SAMPLEFZ350
Max Number of Admin Domains : 4000
Admin Domain Configuration : Disabled
FIPS Mode : Disabled
Branch Point : 738
```

```
Release Version Information : GA
Current Time : Tue Feb 23 10:22:53 PST 2016
Daylight Time Saving : Yes
Time Zone : (GMT-8:00) Pacific Time (US & Canada).
x86-64 Applications : Yes
Disk Usage : Free 17020.10GB, Total 40314.71GB
File System : Ext4
```

Line	Notes
`Current Time`	This is the SQL insert start time.
`File System`	Ensure the file system is `Ext4`. Other file systems will likely cause performance issues.

Possible Solutions

- The `Version` line shows the software version. Ensure you are running the latest software version.
- Check the hardware `Platform Type`. Consider upgrading older hardware, especially older hardware running newer software such as v5.2 or later.
- Ensure `File System` is `Ext4`. Other file systems will likely cause performance issues.

Run `diagnose fortilogd lograte`

This command shows the log receive rate.

Following is a sample result of running this command.

```
logs/sec: 121091.0, logs/30sec: 119613.9, logs/60sec: 116695.8
```

Possible Solutions

- If the log rate is higher than the sustained rates for your FortiAnalyzer model, consider upgrading the hardware. See the Data Sheet on the FortiAnalyzer web page for the sustained rates for your FortiAnalyzer model.

Check Report and Chart Settings

Resolving hostnames usually takes a long time. If the DNS server is slow or does not support reverse DNS, report generation might hang. Check that `Resolve Hostname` is disabled:

- In *Reports* > *Advanced Settings*, check that `Resolve Hostname` is not selected.
- In the *Chart Library*, check that `Resolve Hostname` is set to `Disabled`.

If you do not need to show all results, specify a lower maximum number of entries:

- In the *Chart Library*, check that the chart's `Show Top (0 for all results)` is not set too high. Setting this field to `0` for all results causes FortiAnalyzer to list all logs for the chart.

Check for crashed daemons

Run `diagnose debug crashlog read` and check for crashed daemons.

Possible Solutions

- If daemons frequently crash, contact customer support for assistance.

Check if report auto-cache is enabled

Run `show system report auto-cache`

This command shows non-default settings in the report auto-cache.

If auto-cache is enabled (default), running `show system report auto-cache` returns nothing.

If auto-cache is disabled, this command returns the following:

```
config system report auto-cache
   set status disable
end
```

To enable report auto-cache:

```
config system report auto-cache
   set status enable
end
```

Possible Solutions

- Ensure auto-cache is enabled.

Check if report auto-cache is enabled for a specific report

Run `execute sql-report list-schedule <ADOM>`

This command shows a summary table of all configured reports with their configuration status.

Following is a sample result of running this command.

```
NAME   SCHEDULED  AUTO-CACHE  REPORT GROUP      REPORT TITLE
================================================================================
1      -          -           -                 Security Analysis
10000  -          -           -                 User Security Analysis
10001  -          -           -                 Application and Risk Analysis
10002  -          -           -                 Bandwidth and Applications Report
10003  -          -           -                 Email Report
10004  -          -           -                 Admin and System Events Report
10005  -          -           -                 User Report
10006  -          -           -                 Threat Report
10007  -          -           -                 IPS Report
10008  -          -           -                 Detailed Application Usage and Risk
10009  -          -           -                 Top 20 Categories and Applications (Bandwidth)
10010  -          -           -                 Top 20 Categories and Applications (Session)
10011  -          -           -                 Top Allowed and Blocked with Timestamps
10012  -          -           -                 User Detailed Browsing Log
10013  -          -           -                 Hourly Website Hits
10014  -          -           -                 Top 20 Category and Websites (Bandwidth)
10015  -          -           -                 Top 20 Category and Websites (Session)
10016  -          -           -                 Top 500 Sessions by Bandwidth
10017  -          -           -                 User Top 500 Websites by Bandwidth
10018  -          -           -                 User Top 500 Websites by Session
2      -          -           -                 Client Reputation
3      -          -           -                 Wireless PCI Compliance
4      -          -           -                 VPN Report
5      -          -           -                 Web Usage Report
6      V          V           -                 Microsoft Puget Sound Traffic Report
60012  -          -           -                 Template - User Detailed Browsing Log
60017  -          -           -                 Template - User Top 500 Websites by Bandwidth
60018  -          -           -                 Template - User Top 500 Websites by Session
60019  -          -           -                 Template - Application Risk and Control
7      -          -           -                 WiFi Network Summary
8      V          V           -                 EDGE Microsoft Puget Sound Traffic Report
9      V          V           -                 OpenWiFi Microsoft Puget Sound Traffic Report
```

Possible Solutions

- Check the `AUTO-CACHE` column. Ensure auto-cache is enabled for the main reports, especially scheduled reports. See How auto-cache works in the *FortiAnalyzer Administration Guide*.

Check and adjust report auto-cache daemon

Run `get system performance`

This command shows system performance statistics such as CPU, memory, and I/O usage.

Following is a sample result of running this command.

```
CPU:
   Used:                 49.51%
   Used(Excluded NICE):  49.51%
        %used  %user  %nice  %sys  %idle %iowait  %irq %softirq
   CPU0 27.89  20.60   0.00  5.40  96.42    0.80   0.00     1.79
   CPU1 21.62  12.61   0.00  8.20  98.38    0.40   0.00     0.40
Memory:
   Total:  6,134,200 KB
   Used:   3,770,260 KB   61.5%
Hard Disk:
   Total:   82,434,736 KB
   Used:    65,283,648 KB  79.2%
   IOStat:  tps r_tps w_tps r_kB/s w_kB/s queue wait_ms  svc_ms %util sampling_sec
            4.7   0.2   4.4   27.5  144.2   0.2    52.5     8.4   3.9    599578.78
Flash Disk:
   Total:   499,656 KB
   Used:    314,416 KB     62.9%
   IOStat:  tps r_tps w_tps r_kB/s w_kB/s queue wait_ms  svc_ms %util sampling_sec
            0.0   0.0   0.0    0.0    0.0   0.0    13.6     4.6   0.0    599578.78
```

Following is a sample result of high `%iowait`.

```
FAZVM64 # [530] iowait usage (27.5%) is over limit (23%).
[530] iowait usage (25.9%) is over limit (23%).
[530] iowait usage (28.3%) is over limit (23%).
```

Possible Solutions

- Check the `Used` and `IOStat` lines to see if I/O is busy.
- If both CPU `%used` and `%iowait` are high, check if the report cache daemon is running:
  ```
  diagnose debug enable
  diagnose debug application sqlrptcached 8
  ```
- If a message shows that `sqlrptcached` is stopped, do one or both of the following:
  - Change the report schedule to run at a less busy time. To see scheduled reports, run `execute sql-report list-schedule <ADOM>`. To configure report schedules, see Report configuration in the *FortiAnalyzer Administration Guide*.
  - Enable `aggressive-schedule` so the report auto-cache daemon does not stop even under heavy system load:
    ```
    config system report auto-cache
      set aggressive-schedule enable
    end
    ```

Check and adjust report hcache

Run `diagnose test application sqlrptcached 2`

This command shows if hcache creation is able to catch up.

Following is a sample result of running this command.

```
Number of log table read: all=6453(fortiview=0, rpt=6453) pending=1
Number of log table done: all=6453(fortiview=0, rpt=6453) rpt=6453
Current hcache table entries: 155750
Number of hcache requests sent: 70999
Number of log table vacuums: 39401, pending=2
FortiView hcache load: rounds=817, tbl=653600
ncmdb:
cache hit: sch=0, config=27, chart=140, macro=0, dataset=140 config=27
calls : sch=130, config=11, chart=23, macro=0, dataset=23
```

The following table provides notes about some output lines in the example.

Line	Notes
`Number of log table read`	A high `pending` number indicates the system lacks resources to create cache.
`Number of log table done`	The number of master tables used to calculate the `Number of hcache requests sent`.
`Current hcache table entries`	Total hcache on the system.
`Number of hcache requests sent`	The number of charts per report * the number of master tables * the number of reports.
`Number of log table vacuums`	The postgres built-in status. A high `pending` number indicates postgres resource issues.
`FortiView hcache load`	`rounds` number indicate the number of FortiView caches proactively loaded into memory.
`ncmdb`	Report configuration database.
`cache hit`	`config` is the number of enabled auto cache.

Possible Solutions

- A high `pending` number indicates there are too many pending log tables to read. In this case, consider disabling auto-cache on some reports. See How auto-cache works in the *FortiAnalyzer Administration Guide*.

- Run `execute sql-report list-schedule <ADOM>` and check if there are too many scheduled reports and if auto-cache is enabled. To change report configuration, see Configuration tab in the *FortiAnalyzer Administration Guide*.
- Run `execute top` to check which applications are using the most system resources.

Run `diagnose sql status sqlreportd`

This command shows SQL query connections and hcache status.

Before running this command, enable debug messages: `diagnose debug enable`.

Following is a sample result of running this command.

```
PID: 671
Thread registered: 6
cur_conn_from: code=6 ddown=0 cli=0 gui=0 quota=0
req_conn_from: code=5 ddown=0 cli=0 gui=0 quota=0
db_conn_from: code=5 ddown=0 cli=0 gui=0 quota=0
close_conn: idle=2415 threshold=0 all_threshold=0

query cache: ver=x64_01
query cache: hash-tbl=29947 entries=816 est-bytes=4241568
query cache: query=1558 hit=783 make=816 del=0 dirty=0 save=776 load=42

hcache: sche-create=1982 sche-hits=89088
        ddown-create=24 ddown-hits=4
        autocache-create=73471 autocache-hits=186204
```

The following table provides notes about some output lines in the example.

Line	Notes
`hcache`	A high `sche-hits` indicates that report cache is used.
`ddown-create`	A high `ddown-hits` indicates that FortiView cache is used.

Possible Solutions

- If both `sche-create` and `sche-hits` are low, ensure that reports are scheduled and auto-cache is enabled. To check report configuration, run `execute sql-report list-schedule <ADOM>`. To change report configuration, see Configuration tab in the *FortiAnalyzer Administration Guide*.

Run `execute sql-report hcache-check <ADOM> <schedule-id>`

This command shows a specific report's hcache status.

If necessary, check the hcache status of a specific report that you think might be a problem.

For example, if the `ADOM` is `root` and `schedule-id` is `10004`, then run `execute sql-report hcache-check root 10004`.

To get the `schedule-id`, run `execute sql-report list-schedule root` and see the `NAME` column.

Following is a sample result of running the `execute sql-report hcache-check <ADOM> <schedule-id>` command.

```
layout_num:1
start [0] get layout-id:10004.
start report_process, layout-id:10004, layout title:Admin and System Events Report.
device list:All_FortiGates.
reports num:1.
device list[0].FWF60C3G13006291[root].
device list[1].FG3K2C3Z11800039[root].
......
> checking (10004_t10004-Admin and System Events Report) ...
checking chart Admin-Login-Summary...
8/8 (100%) done 0.131 secs used.
checking chart Admin-Login-Summary-By-Date...
8/8 (100%) done 0.128 secs used.
...
```

Possible Solutions

- If a few reports are causing a bottleneck, reconfigure those reports. See these sections in the *FortiAnalyzer Administration Guide*: *Check if report auto-cache is enabled for a specific report*, *Check and adjust report auto-cache daemon*, and *Check and adjust report hcache*.

Summary of commands for troubleshooting report performance

The following is a summary of troubleshooting commands used in this appendix.

CLI	Notes
`get system status`	This command shows system status such as platform type (hardware or VM), firmware version, system time, disk usage, and file system format.
`get system performance`	This command shows system performance statistics such as CPU, memory, and I/O usage.
`show system report auto-cache`	This command shows non-default settings in the report auto-cache.
`execute sql-report hcache-check <ADOM> <schedule-id>`	This command shows a specific report's hcache status.
`diagnose fortilogd lograte`	This command shows the log receive rate.
`diagnose debug enable`	This command enables debug messages to run SQL diagnostic commands.
`diagnose sql show hcache-size`	This command shows the hcache size.
`diagnose sql status sqlreportd`	This command shows SQL query connections and hcache status.
`diagnose debug application sqlrptcached 8`	This command sets the debug level of the SQL report cache daemon.
`diagnose debug disable`	This command disables debug message.
`diagnose test application sqlrptcached 2`	This command shows if hcache creation is able to catch up.
`execute sql-report list-schedule <ADOM>`	This command shows a summary table of all configured reports with their configuration status.
`execute top`	This command shows the processes running on the FortiAnalyzer system.
`diagnose debug crashlog read`	This command prints information of all crashed daemons.